

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété
Intellectuelle
Bureau international



(43) Date de la publication internationale
27 janvier 2005 (27.01.2005)

PCT

(10) Numéro de publication internationale
WO 2005/008951 A2

(51) Classification internationale des brevets⁷ : **H04L 9/08**

(21) Numéro de la demande internationale :
PCT/FR2004/001362

(22) Date de dépôt international : 2 juin 2004 (02.06.2004)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
0307287 17 juin 2003 (17.06.2003) FR

(71) Déposant (pour tous les États désignés sauf US) :
FRANCE TELECOM [FR/FR]; 6, Place d'Alleray,
F-75015 PARIS (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : **ARDITTI**

MODIANO, David [FR/FR]; 46ter, rue Paul Vail-
lant-Couturier, F-92140 CLAMART (FR). **BILLET,**
Olivier [FR/FR]; 1211 Route des Vallettes Sud, F-06140
TOURRETTES/LOUP (FR). **GILBERT, Henri** [FR/FR];
2, allée des Peupliers, F-91440 BURES SUR YVETTE
(FR).

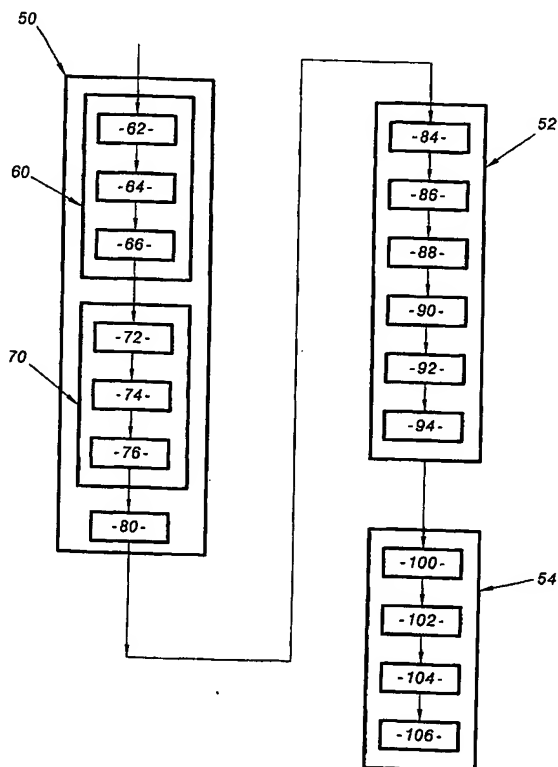
(74) Mandataires : **DOMENEGO, Bertrand** etc.; CABINET
LAVOIX, 2, place d'Estienne d'Orves, F-75441 PARIS
CEDEX 09 (FR).

(81) États désignés (sauf indication contraire, pour tout titre de
protection nationale disponible) : AE, AG, AL, AM, AT,
AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO,
CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB,
GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG,
KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG,

[Suite sur la page suivante]

(54) Title: TRACEABLE METHOD AND SYSTEM FOR ENCRYPTING AND/OR DECRYPTING DATA, AND RECORDING
MEDIA THEREFOR

(54) Titre : PROCEDE ET SYSTEME TRACABLES DE CHIFFREMENT ET/OU DE DECHIFFREMENT D'INFORMATIONS,
ET SUPPORTS D'ENREGISTREMENT POUR LA MISE EN OEUVRE DU PROCEDE



(57) Abstract: The invention concerns a traceable method for en-
crypting and/or decrypting data broadcast by at least one trans-
mitter towards several decoders wherein: during encryption of
broadcast data, the transmitter implements (in 86) at least one first
secret function to transform an unencrypted message into an en-
crypted message; and during decryption of said broadcast data, all
the decoders implement (in 92) at least one common second secret
function, each decoder using therefor a mathematical description
of the second function stored in a memory (21), the mathematical
description of said second function being different from one de-
coder to another or from one group of decoders to another such
that the mathematical description used identifies exclusively the
particular decoder or group of decoders.

(57) Abrégé : L'invention concerne un procédé traçable de
chiffrement et/ou de déchiffrement d'informations diffusées par
au moins un émetteur vers plusieurs décodeurs dans lequel : -
lors du chiffrement des informations diffusées, l'émetteur met
en œuvre (en 86) au moins une première fonction secrète pour
transformer un message non chiffré en un message chiffré, et
- lors du déchiffrement de ces informations diffusées, tous les
décodeurs mettent en œuvre (en 92) au moins une même seconde
fonction secrète, chaque décodeur faisant appel à cet effet à une
description mathématique de ladite seconde fonction enregistrée
dans une mémoire (21), la description mathématique de cette
seconde fonction étant différente d'un décodeur à l'autre ou d'un
groupe de décodeurs à l'autre de manière à ce que la description
mathématique à laquelle il est fait appel identifie de façon unique
le décodeur ou un groupe de décodeurs particulier.

WO 2005/008951 A2



MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Publiée :

— sans rapport de recherche internationale, sera republiée dès réception de ce rapport

(84) États désignés (sauf indication contraire, pour tout titre de protection régionale disponible) : ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), eurasién (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI,

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.